

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-161321

(43)Date of publication of application : 18.06.1999

(51)Int.Cl.

G05B 23/02

G06F 3/14

G06F 13/00

G06F 17/60

(21)Application number : 09-327981

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 28.11.1997

(72)Inventor : INUBUSHI HIROYUKI

## (54) PLANT MONITOR DEVICE

(57)Abstract:

**PROBLEM TO BE SOLVED:** To provide the plant monitor device which transmits plant data from a remote plant by a desired computer and disables access from a person, a place, and a computer that are not allowed.

**SOLUTION:** This device has a data input part 2 which inputs data from a plant 1, a server 10 which inputs the data of the plant 1 from the data input part 2 and outputs them to the internet 20 or an intranet, and a computer 30 which is connected to the internet or intranet and inputs the data of the plant 1 sent from the sever 10, and the server 10 is equipped with a ciphering means which ciphers and outputs the plant data and outputs the data to a firewall for preventing illegal access from the internet 20.



## LEGAL STATUS

[Date of request for examination]

27.01.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-161321

(43) 公開日 平成11年(1999) 6月18日

(51) Int.Cl.<sup>8</sup>  
G 0 5 B 23/02  
G 0 6 F 3/14  
13/00  
17/60

識別記号  
3 2 0  
3 5 5

F I  
G 0 5 B 23/02 V  
G 0 6 F 3/14 3 2 0 C  
13/00 3 5 5  
15/21 Z

審査請求 未請求 請求項の数6 O L (全 5 頁)

(21) 出願番号 特願平9-327981

(22) 出願日 平成9年(1997)11月28日

(71) 出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72) 発明者 犬伏 裕之

東京都府中市東芝町1番地 株式会社東芝  
府中工場内

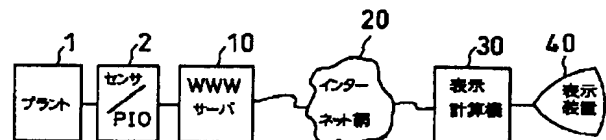
(74) 代理人 弁理士 外川 英明

(54) 【発明の名称】 プラント監視装置

(57) 【要約】

【課題】 遠隔のプラントからプラントデータを所望の計算機にて伝送し、利用を許可していない者、場所、計算機からのアクセスを出来ないようなプラント監視装置を提供する。

【解決手段】 プラントのデータを入力するデータ入力部と、このデータ入力部からプラントのデータを入力し、インターネット網あるいはイントラネット網に出力するサーバと、インターネット網あるいはイントラネット網に接続され、前記サーバから送信されるプラントのデータを取り込む計算機とを有し、サーバはプラントデータを暗号化して出力する暗号化手段を備えたり、インターネット網からの不正なアクセスを防止するファイアウォールに出力する。



## 【特許請求の範囲】

【請求項1】 プラントのデータを入力するデータ入力部と、このデータ入力部からプラントのデータを入力し、インターネット網あるいはイントラネット網に出力するサーバと、インターネット網あるいはイントラネット網に接続され、前記サーバから送信されるプラントのデータを取り込む計算機とを有することを特徴とするプラント監視装置。

【請求項2】 請求項1のプラント監視装置において、前記サーバはプラントデータを暗号化して出力する暗号化手段を備え、前記計算機は送信されるデータを復号化する復号化手段を備えることを特徴とするプラント監視装置。

【請求項3】 プラントのデータを入力するデータ入力部と、前記データ入力部からプラントのデータを入力し、インターネット網からの不正なアクセスを防止するファイアウォールに出力するサーバと、インターネット網に接続され、前記サーバから送信されるプラントのデータを前記ファイアウォールを介して取り込む計算機とを有することを特徴とするプラント監視装置。

【請求項4】 プラントのデータを入力するデータ入力部と、前記データ入力部からプラントのデータを入力し、インターネット網からの不正なアクセスを防止する第一のファイアウォールに出力するサーバと、インターネット網に接続される第二のファイアウォールに接続され、前記サーバから送信されるプラントのデータを前記第二のファイアウォールから取り込む計算機とを有することを特徴とするプラント監視装置。

【請求項5】 請求項3または請求項4のプラント監視装置において、前記ファイアウォールは、VPN機能を備えることを特徴とするプラント監視装置。

【請求項6】 請求項1、3または4のプラント監視装置において、前記計算機は、利用者を特定するセキュリティ機能を有し、当該セキュリティ機能の確認によりプラントのデータの取り込みあるいは表示を可能とするものであることを特徴とするプラント監視装置。

## 【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明はインターネット網あるいはイントラネット網を用いたプラント監視装置に関する。

【0002】

【従来の技術】 工業プラント、発電プラント、電力系統等のプラントでは、図9のように、ある程度距離が離れると、伝送装置を用いて、プラントのデータを伝達している。図中センサ／PIOは、一つの形態であってプラント監視の対象がデジタル化されている場合は、単にデータ入力装置となる場合もある。

【0003】 また、遠隔地からの監視をする場合には、従来では、専用回線を用いたりISDNを利用するのが

一般的であった。発電プラント等でも、発電所と本店間の監視には、専用回線を使用している。この専用回線やISDNの利用では、コスト高となる問題がある。

【0004】 しかし、従来はインターネットの技術がなかったことまた、インターネット自体は、ビジネス向けに、比較的静的な情報（変化がゆっくりとしたもの）を表示していることから、プラント情報のようにたえず変化する動的な情報を伝送表示するという発想がなかった。

【0005】 また、表示しようとしても、例えば発電所のようなデータをインターネットを用いて表示するには、以下の様な問題がありその実現は難しかった。

(1) インターネットは、データが網の目の様にはりめぐらされたネットワークを、途中にあるサーバを経由しながら伝送されていくため、途中のサーバで、そのデータを盗聴しようと考えれば、可能である。

(2) インターネットは、世界中に広がるネットワークであるので、URLと呼ばれるインターネットのWWWサーバのアドレスが知られてアクセスされると、第三者に容易に中味を見られてしまう。

(3) 仮にある端末（表示装置）のみから見られるようににしても、その端末に近づくことができれば、利用を許可していない人でも、電源を入れて表示装置から情報を見ることも可能であった。

【0006】 このように、利用を許可していない人間からデータを守るために、セキュリティを強化する必要があったが、これに必要な技術をうまく組み合わせて利用することができなかった。

【0007】

【発明が解決しようとする課題】 そこで、本発明では、利用を許可していない人、場所からは、容易にデータを見ることができない様な、プラント監視装置を提供することを目的とする。

【0008】

【課題を解決するための手段】 本発明のプラント監視装置は、プラントのデータを入力するデータ入力部と、このデータ入力部からプラントのデータを入力し、インターネット網あるいは、イントラネット網に出力するサーバと、インターネット網あるいはイントラネット網に接続され、前記サーバから送信されるプラントのデータを取り込む計算機とを有する。

【0009】 そして、このプラント監視装置のサーバはプラントデータを暗号化して出力する暗号化手段を備え、計算機は送信されるデータを復号化する復号化手段を備える。

【0010】 また、本発明のプラント監視装置は、プラントのデータを入力するデータ入力部と、前記データ入力部からプラントのデータを入力し、インターネット網からの不正なアクセスを防止するファイアウォールに出力するサーバと、インターネット網に接続され、前記サ

3

サーバから送信されるプラントのデータを前記ファイアウォールを介して取り込む計算機とを有する。

【0011】また、プラントのデータを入力するデータ入力部と、前記データ入力部からプラントのデータを入力し、インターネット網からの不正なアクセスを防止する第一のファイアウォールに出力するサーバと、インターネット網に接続される第二のファイアウォールに接続され、前記サーバから送信されるプラントのデータを前記第二のファイアウォールから取り込む計算機とを有する。

【0012】そして、このファイアウォールは、VPN機能を備える。また、本発明のプラント監視装置において、前記計算機は、利用者を特定するセキュリティ機能を有し、当該セキュリティ機能の確認によりプラントのデータの取り込みあるいは表示を可能とするものである。

【0013】

【発明の実施の形態】以下、本発明の実施の形態について、図面を参照して説明する。図1は、本発明の最も基本的な技術的思想を示すものである。第1実施の形態の図1は、従来の図9の専用回線120の代りに、インターネット網20を用いている点が大きく異なる。また、図9では、専用回線120の両端は伝送装置110と130であるのに対して、図1ではWWWサーバ10と表示計算機30である。WWWサーバ10は、インターネットを実現するデータをもっているところである。一方、表示計算機30は一般にパソコンで実施している。

【0014】データ入力部のセンサ／PIO2は、プラント1からのデータをを入力する。WWWサーバ10は、前記センサ／PIO2が入力したデータを、入力処理し、インターネットで利用できるデータ形式に処理を行い、インターネット網20に出力する。

【0015】表示計算機30では、このデータを入力して、プラント状態を表示装置40に表示する。次に、第2の実施の形態を図2について説明する。

【0016】第1実施形態の場合は、インターネット網を使うため、セキュリティの問題がある。そこで、インターネット網の代りに、イントラネット網を用いる。インターネットが公衆の網であるのに対して、イントラネットは、企業内の専用の網である。従って、専用回線を用いたのと同じになるため、社外のメンバからの不正アクセスは阻止できる。

【0017】次に、第3の実施の形態を図3について説明する。網は、インターネット網を使うが、ファイアウォールという情報の防火壁を設けることにより、不正なアクセスを防止することができる。

【0018】次に、第4の実施の形態を図4について説明する。基本的には図1と同じであるが、WWWサーバと、表示計算機に暗号化プロトコルが組み込まれている点が異なる。「暗号化プロトコルとは、OSI参照でい

4

う、物理層、ネットワーク層、セクション層、アプリケーション層で主に用いられているプロトコルで、その代表的なものがSSLである。」SSL (Secure Sockets Layer) は、サーバと、WWWブラウザのためにセキュリティ機構として、W3Cワーキンググループのセキュリティ部門によって提案された通信方式である。これは、通信において特定のある部分だけを暗号化するのではなく、インターネットの基本的なプロトコルであるTCP/IPで通信される内容の全てを暗号化するものである。SSLの場合、通常WWWブラウザに組み込まれるため、使用者は意識する必要がない。

【0019】また、WWWサーバと表示計算機時間のデータが全て暗号化されているので仮に、この間で流れているデータが盗まれても、盗んだ人は解読できないので、実用上、問題ない。現在、SSLに類似のものである、PCT (Private Communication Technology) 等がある。

【0020】次に、第5の実施の形態の図5について説明する。図3のファイアウォールにさらに、VPN (バーチャルプライベートネットワーク) の機能をもたせたものである。VPNも、前述のSSLと同様に暗号化する機能があり、さらに、トンネリング機能という機能も同時に実現する。このトンネリング機能とは、予め決められたトンネル (経路) でしか、インターネットがアクセスできないようにする機能である。

【0021】つまり、「経路」は、IPアドレスという固有の接続点で識別され、当該のIPアドレスをもった利用者からしかアクセスできないようになる。これにより、従来の問題点の「許可している場所」以外からのアクセスはシャットアウトすることができる。

【0022】一般に、VPNの機能はファイアウォールにもたせている。この実施例では、暗号化されたデータを復号化するために表示計算機側にもVPN機能付きのファイアウォールを設けている。

【0023】次に、第6の実施の形態の図6について説明する。第5実施によると、特定の端末からでないと利用できないとしても、その端末に近づくことができる人であれば、電源を入れて表示装置を生かし、表示端末からデータが自由にひき出してしまう。そこで、表示計算機にICカード読みとり機をつけて、予め登録してあるICカードを使用する人からしか、表示計算機がさわれないようにするものである。ここでは、ICカードとしているが、これに類する磁気カード等でも同様に扱えることは言うまでもない。

【0024】次に、第7の実施の形態を図7について説明する。図6では、操作する人が妥当か否かをICカードという本人が所持しているものを用いて判定した。

【0025】一方、図7では、ICカードの代りに、操作する人のバイオメトリクス (生体情報) を用いる。バイオメトリクスとは、個人の身体的特徴 (指紋や掌紋

10

20

30

40

50

等)や、個人の行為(筆跡、声紋)を用いて、本人であるかを識別することをさす。考え方は、図6と同様である。予め本人データを登録しておき、このデータと、バイオメトリクスセンサ経由で入力されたデータが一致したら、表示用計算機のアクセスを許可する。バイオメトリクスのために指紋を用いれば、バイオメトリクスセンサは“指紋読みとり器”となる。

【0026】次に、第8の実施の図8について説明する。これは、図6とほぼ同様であるが、ICカードの代りに、本人のID番号と、このID番号に対応するパスワードを使うものである。アクセスを開始する際に、操作する人は、ID番号とパスワードを入れなければ、中味を見ることができない。ごく簡単なやり方としては、この図8の装置で実現できるが、インターネット網を流れるデータは、暗号化されていないので、クラッカー(ハッカー)と呼ばれる悪意をもった人からは、簡単にID番号と、パスワードが盗まれるという欠点はある。

【0027】従って、実際には図8は、暗号化技術を使用する図4、図5の装置方法と組合せて実現することになる。尚、ID番号は、1人ずつ違うものを割りあてておく。またアクセス記録は定期的にチェックし、本人からのアクセスであるかをチェックすることができる。

【0028】以上のように、発明によれば、従来専用の通信回線を、設けなければ実現できなかったものが、インターネット網により簡単に遠隔の監視を行うことができ、通信回線が不要となる。その結果、大幅なコストの削減も可能になる。具体的なコストは、距離等によるので、一概には言えないが、専用回線を確立するには、100万円～1000万円オーダー以上の費用がかかる。これに対し、インターネット網が利用できればこのコストの1/10～1/100以下のコストで通信が可能と考えられる。また、計算機の設置場所の変更、増設についても対応が容易にできる。

【0029】また、不正アクセス者が、WWWサーバのURLを知れば簡単に見られる危険があったものが、ファイアウォールにより、予め登録されたアクセス者またはアクセス装置からの接続しか許可しないため、より安全に通信を行うことが可能となる。

【0030】また、通信網上のデータが暗号化されていないので、クラッカー等からデータ自体の盗聴をされると、そのまま内容が流出してしまうことになっていたものが、暗号化により見られても内容までは解読できないことにより、セキュリティを確保することが可能となる。

【0031】また、本発明によれば、VPNの機能により、データが暗号化されるとともに、トンネリングの機

能により“許可している場所(IPアドレス)”以外からのアクセスをシャットアウトすることが可能となる。

【0032】また、本発明によれば、ICカードを所持した人間からしかアクセスが許可されないの、不正なアクセスを防止することができる。例えば、請求項5を適用しても、電源を入れてその端末からアクセスされてしまう可能性があったが、このICカードを用いれば、当該のICカードを所持している請求項7の発明によれば、バイオメトリクス(指紋等)が一致した人間からしかアクセスが許可されないの、不正なアクセスを防止することができる。

【0033】また、本発明によれば、ID番号とパスワードを知っている人からしかアクセスできないの、不正なアクセスを防止することができる。また、何らかの方法で不正アクセス者が、ID番号とパスワードを盗んでしまっても、少くともアクセス記録は残るので、これをもとに不正アクセス者を割り出すことができる等の効果も期待できる。

【0034】

【発明の効果】本発明によれば、遠隔のプラントのデータを簡単かつ安全に送信できるプラント監視装置を提供できる。

【図面の簡単な説明】

【図1】本発明の第1の実施形態のプラント監視装置の構成図

【図2】本発明の第2の実施形態のプラント監視装置の構成図

【図3】本発明の第3の実施形態のプラント監視装置の構成図

【図4】本発明の第4の実施形態のプラント監視装置の構成図

【図5】本発明の第5の実施形態のプラント監視装置の構成図

【図6】本発明の第6の実施形態のプラント監視装置の構成図

【図7】本発明の第7の実施形態のプラント監視装置の構成図

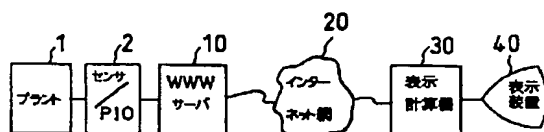
【図8】本発明の第8の実施形態のプラント監視装置の構成図

【図9】従来のプラント監視装置の構成図である。

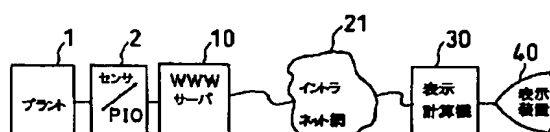
【符号の説明】

1…プラント、2…データ入力部(センサ/PIO)、10、13…WWWサーバ、11、12、32…ファイアウォール、20…インターネット網、21…イントラネット網、30、31…計算機、40…表示装置

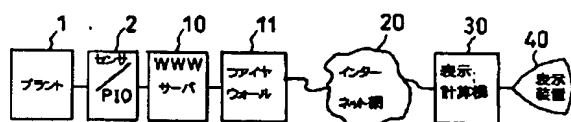
【図1】



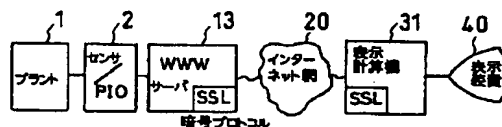
【図2】



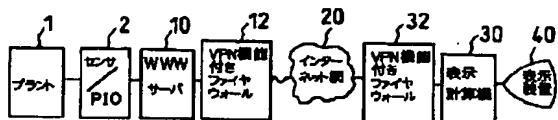
【図3】



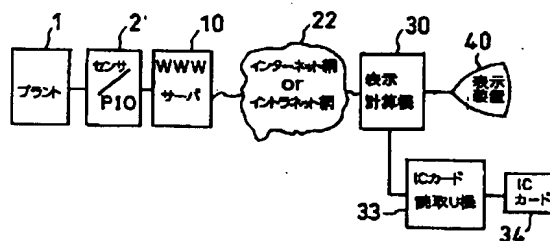
【図4】



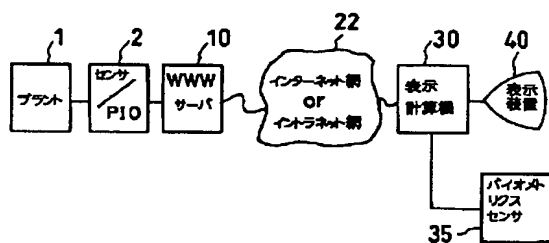
【図5】



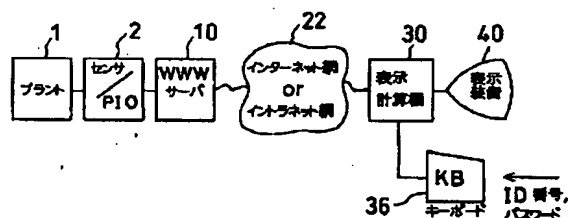
【図6】



【図7】



【図8】



【図9】

